## AMENDMENTS TO THE CLAIMS

The listing of claims will replace all prior versions, and listings, of claims in the application:

**Listing of Claims:**

1. (Currently Amended) In a network system that includes a first computer system network connectable to a second computer system, the first computer system capable of encrypting data, a method of the first computer system encrypting data so as to guard against eavesdropping and brute force attacks, the method comprising the following:

an act of securely negotiating a master secret with the second computer system for a plurality of data packets to be transmitted from the first computer system to the second computer system;

an act of generating a random bit sequence for each data packet, the random bit sequence being different for each data packet;

an act of including the random bit sequence, for each data packet, into a seed to generate a random seed that is different for each data packet;

for each data packet, an act of inputting the master secret and the random seed corresponding to each data packet into a key generation module to generate a corresponding key, such that the corresponding key is different for each data packet;

for each data packet, an act of using the corresponding key to encrypt the corresponding data packet; and

for each data packet, an act of including the encrypted data packet and the corresponding random seed in a data structure that is transmitted form the first computer to the second computer.

2. (Original) A method in accordance with Claim 1, wherein the data structure is a data packet, the method further comprising an act of transmitting the data packet in accordance with a protocol.

3. (Original) A method in accordance with Claim 2, wherein the data packet includes a Security Parameter Index in accordance with the Encapsulating Security Payload (ESP) protocol.

4. (Cancelled).

5. (Original) A method in accordance with Claim 2, wherein the protocol comprises an unconfirmed push protocol.

6. (Original) A method in accordance with Claim 5, wherein the unconfirmed push protocol comprises User Datagram Protocol (UDP).

7. (Original) A method in accordance with Claim 1, further comprising an act of negotiating a parameter expiry with the second computer system, the parameter expiry indicating the lifetime of the master secret.

8. (Original) A method in accordance with Claim 7, wherein upon expiration of the lifetime of the master secret, performing an act securely renegotiating a master secret with the second computer system.

9. (Original) A method in accordance with Claim 1, wherein the second computer system comprises a wireless device.

10. (Original) A method in accordance with Claim 1, wherein the act of generating a random bit sequence is performed by a cryptographically secure random number generator.

11. (Original) A method in accordance with Claim 1, further comprising an act of including, in the random seed, a bit sequence that represents the current time.

12. (Original) A method in accordance with Claim 1, wherein the random seed is at least 96 bits.

13. (Currently Amended) A computer program product for use in a network system that includes a first computer system network connectable to a second computer system, the computer program product for implementing a method of the first computer system encrypting data so as to guard against eavesdropping and brute force attacks, the computer program product comprising a computer-readable medium having stored thereon the following:

computer-executable instructions for performing an act of securely negotiating a master secret with the second computer system for a plurality of data packets to be transmitted from the first computer system to the second computer system;

computer-executable instructions for performing an act of generating a random bit sequence for each data packet, the random bit sequence being different for each data packet;

computer-executable instructions for performing an act of including the random bit sequence, for each data packet, into a seed to generate a random seed that is different for each data packet;

computer-executable instructions for performing, for each data packet, an act of inputting the master secret and the random seed corresponding to each data packet into a key generation module to generate a corresponding key, such that the corresponding key is different for each data packet;

computer-executable instructions for performing, for each data packet, an act of using the corresponding key to encrypt the corresponding data packet; and

computer-executable instructions for performing, for each data packet, an act of including the encrypted data packet and the corresponding random seed in a data structure that is transmitted form the first computer to the second computer.

14. (Original) The computer program product as recited in Claim 13, wherein the computer-readable medium is a physical storage medium.

15. (Currently Amended) In a network system that includes a first computer system network connectable to a second computer system, the first computer system capable of encrypting data, a method of the first computer system encrypting data so as to guard against eavesdropping and brute force attacks, the method comprising the following:

an act of securely negotiating a master secret with the second computer system;

a step for generating a different encryption key, for each corresponding data packet transmitted between the first and second computer systems, using the master secret and ~~the~~ a different random seed for each data packet~~so that the master secret and key are difficult for an eavesdropper to identify~~;

an act of using the different encryption keys to encrypt the corresponding data packets~~the key to encrypt data~~; and

an act of ~~including~~ transmitting the encrypted data packets to the second computer system, each data packet being transmitted with ~~and~~ the different random seed that was used to generate the encryption key corresponding to each data packet~~in a data structure~~.

16. (Original) A method in accordance with Claim 15, wherein the data structure is a data packet, the method further comprising an act of transmitting the data packet in accordance with a protocol to the second computer system.

17. (Cancelled).

18. (Original) A method in accordance with Claim 16, wherein the protocol comprises an unconfirmed push protocol.

19. (Original) A method in accordance with Claim 18, wherein the unconfirmed push protocol comprises User Datagram Protocol (UDP).

20. (Original) A method in accordance with Claim 15, wherein the second computer system comprises a wireless device.

21. (Original) A method in accordance with Claim 15, further comprising an act of including, in the random seed, a bit sequence that represents the current time.

22. (Original) A method in accordance with Claim 15, wherein the step for generating a key using the master secret and the random seed comprises the following:

an act of generating a random bit sequence;

an act of including the random bit sequence in a seed to generate the random seed; and

an act of inputting the master secret and the random seed into a key generation module to generate a key.

23. (Currently Amended) In a network system that includes a first computer system network connectable to a second computer system, a method of the second computer system decrypting a data packet that was transmitted to the second computer system by the first computer system, the data packet being encrypted so as to guard against eavesdropping and brute force attacks, the method comprising the following:

an act of securely negotiating a master secret with the first computer system;

an act of receiving a plurality of encrypted data packets from the first computer system, wherein the first computer system encrypts every data packet with a different key based on a different random seed, such that each encrypted data packet received by the second computer system is encrypted with a different key based;

an act of reading a random seed from at least one of the data packets ~~received from the first computer system, the random seed including a random bit sequence generated by a random number generator~~;

an act of inputting the master secret and the random seed into a key generation module to generate a key; and

an act of using the key to decrypt the data packet.

24. (Original) A method in accordance with Claim 23, wherein the data packet includes a Security Parameter Index in accordance with the Encapsulating Security Payload (ESP) protocol.

25. (Cancelled).

26. (Original) A method in accordance with Claim 23, wherein the data packet is received using an unconfirmed push protocol.

27. (Original) A method in accordance with Claim 26, wherein the unconfirmed push protocol comprises User Datagram Protocol (UDP).

28. (Original) A method in accordance with Claim 23, further comprising an act of negotiating a parameter expiry with the first computer system, the parameter expiry indicating the lifetime of the master secret.

29. (Original) A method in accordance with Claim 28, wherein upon expiration of the lifetime of the master secret, performing an act securely renegotiating a master secret with the first computer system.

30. (Original) A method in accordance with Claim 29, wherein the second computer system comprises a wireless device.

31. (Original) A method in accordance with Claim 23, wherein the random seed includes a bit sequence that represents the current time.

32. (Original) A method in accordance with Claim 23, wherein the random seed is at least 96 bits.

33. (Currently Amended) A computer program product for use in a network system that includes a first computer system network connectable to a second computer system, the computer program product for implementing a method of the second computer system decrypting a data packet that was transmitted to the second computer system by the first computer system, the data packet being encrypted so as to guard against eavesdropping and brute force attacks, the computer program product comprising a computer-readable medium having stored thereon the following:

computer-executable instructions for performing an act of securely negotiating a master secret with the first computer system;

computer-executable instructions for performing an act of ~~detecting the receipt of a data packet from the first computer system~~ receiving a plurality of encrypted data packets from the first computer system, wherein the first computer system encrypts every data packet with a different key based on a different random seed, such that each encrypted data packet received by the second computer system is encrypted with a different key based;

computer-executable instructions for performing an act of reading a random seed from at least one of the data packets ~~received from the first computer system, the random seed including a random bit sequence generated by a random number generator~~;

computer-executable instructions for performing an act of inputting the master secret and the random seed into a key generation module to generate a key; and

computer-executable instructions for performing an act of using the key to decrypt the data packet.

34. (Original) A computer program product in accordance with Claim 33, wherein the computer-readable medium is a physical storage medium.

35. (Currently Amended) In a network system comprising a plurality of server computer system connectable through a network with a plurality of client computer systems, the network system comprising the following:

a server computer system configured to securely negotiate a master secret with a client computer system, generate and include a random bit sequence in a seed to generate a different random seed for every data packet to be transmitted between the client computer systems, input the master secret and ~~the~~ each random seed into a server-side key generation module to generate a different key for every data packet, use ~~the~~ each key to encrypt ~~a~~ the corresponding data packets, and transmit the data packets to the client computer system; and

the client computer system, the client computer system further configured to receive the data packets from the server computer system, read the different random seed from ~~the~~ each data packet, input the master secret and ~~the~~ each different random seed into a client side key generation module to generate ~~a~~ the different keys, and to decrypt the corresponding data packets.